APN GW ™ 5000

使用说明书

Powered by APN GW™ Architecture

深圳市奥联科技发展有限公司



http://www.apn.com.cn

http://www.authcyber.com

APN GW
Installation & Configuration Guide

For APN GW 5000 Series

【Text Part Number: T03-01-12-G12】

Documentation also available on CD-ROM and the Website

声 明

NOTICES

目　　录

关于本手册

目的

本手册提供了 APN GW5000 系列产品安装使用说明。包括硬件安装和系统配置。随 APN 产品系统一起附给用户。

如何使用

本手册分为硬件安装、系统安装、License 管理和系统维护四大部分。使用者可按照本手册所描述，自己完成所有的设置。如没有特别说明，本书中采用的一些标志如下：

内容	含义	描述
注意		表示重点提示，在于某些用户容易误解的内容作出的加重的提示信息。
加粗斜体		表示需要您的输入，其输入内容需要替换成符合您自己系统的具体内容
	警告	表示需要特别注意，许多会跟设备和数据的功能和可靠有关，务必仔细注意
	诀窍	按照该提示可能会使您节约一点时间
	总结	表示对上述内容的一个小结，常常可以使您及时明白上一段所描述内容及其目的。

如何组织

本手册共分为五章。分别介绍了本系统的硬件安装、通过 console 配置、通过 web 配置、局域网设置和常见问题解答五个部分。在安装 5000 服务系统之前，请务必认真阅读。

适用对象

本手册适用于购买我公司 APNGW 5000 系列产品的用户。同时要求使用者需要具有 TCP/IP 的基础知识和一定的网络知识，熟悉电子设备的保护和使用。对 Linux 系统有一定了解。

第一章　硬件安装

本部分主要介绍了 APN GW 的硬件安装。安装正确之后，您就可以进行配置和调试了。

环境要求

系统可在如下的环境下使用。

- 输入电压： 110V~230V
- 功率：最大约 100W
- 使用环境温度：0~35 ℃
- 使用环境湿度：5~95%

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的通风和室温。

安全警告

 本系统不能在有酸性，碱性环境，强磁场等恶劣环境下使用。在这类环境下使用本系统不保证能正常使用。导致的系统物理损坏亦不在本产品的品质保证之中。

 这是甲类的资讯产品，在居住的环境中使用时，可能会造成无线电干扰，在这种情况下，使用者会被要求采取某些适当的措施。

电源

本产品使用交流 100V 到 240V 电源。在您接通电源之前，请保证您的电源有良好的接地。

电脑

在配置本产品之前，您需要配备一个装有超级终端软件的电脑，同时需要该电脑具有至少一个 9 针的 com 接口。如果您运行的是 Microsoft 公司的 Windows 操作系统，您还需要检查是否安装了"超级终端"这个程序。此外，您还可以用一些标准的终端程序，例如 netterm 来进行设置 APN。我们推荐您使用该软件。

如果您需要通过网络进行配置，您的电脑还需要一片网卡。

APN 的背板如下图所示。将 Console 口和一台 PC 机的串口用随机电缆连接起来。

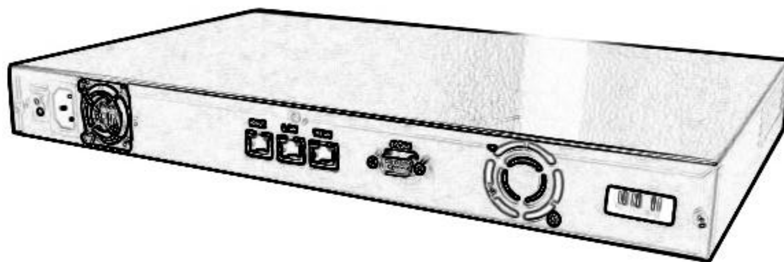


图 2－1 APN GW5000 背板图

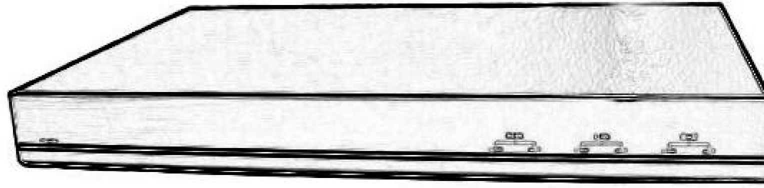


图 2－2 APN GW 5000 面板图

连接 Console 线

用通过 APN 随机带的 RS-232 通讯电缆，把 APN 的系统配置/监控接与控制终端进行互联。

一般用普通电脑作为控制终端。把 Console 电缆一端直接接在 APN GW 背面的 Console 接口上，另外一端连接到电脑的 COM 口上。接线完成后，按下 APN GW 电源开关，配置好终端参数，会看到有关 APN GW 的启动信息和登录提示。

连接局域网

使用标准 RJ-45 插口的以太网接口。

将 APN 的 LAN 端口用 RJ45 网线连接到本地局域网中。

连接广域网

如使用 ADSL 上网，用双绞线与 ADSL CABLE MODEM 上的 LAN 接口连接到 APN GW 产品上标注 Wan 的接口进行互联。

如使用 DDN、Cable Modem、宽带上网的，用双绞线与 APN GW WAN 端口相连。

如果您需要连接 DMZ 区，您可以把您用于对外服务的 WEB 服务器、EMAIL 服务器连接到 DMZ 的接口。

第二章 使用 Console 方式配置 APN

APN GW 支持 Console 配置方式、WEB 配置方式、telnet 配置方式。您可以用超级终端、浏览器来配置。如果您采用浏览器配置方式，您可以不阅读本章直接到下一章。

使用方法和诀窍

我们以 Windows 98 为例。在开始? ? 程序? ? 附件? ? 中，有一个超级终端的软件。您需要启动它。在 APN 和电脑之间，您需要用 console 线连接起来。如果您的 console 线连在电脑的 com3 口上，在超级终端中就需要选择 com3 口。

选择端口后，选择确定，您需要设置通讯的

- 波特率为 9600
- 数据位 8
- 奇偶校验 无
- 停止位 1
- 数据流控制 无



您在设置 APN 的时候，您可以使用 tab 键来完成命令的输入。例如，您需要输入 setup 时，只需要输入 set，然后按 tab 键，系统会自动完成setup 整个字串的键入。这有助于您忘记某些命令时系统自动帮您完成输入。

您在设置 APN 的时候，您可以使用 ctrl 键加 P 键重复上次输入的命令。

基本设置

注意： 以下所列系统显示信息可能会因为 APN 版本的不同而略微有些差异。但以下所列操作适用于所有的版本。

系统正常引导启动(接电源开关并等待约 40 秒左右时间)后。输入配置系统帐号：

Login：***root***

Password：***gw1admin***

系统提示符为 APNGW#。

此时输入 help **可以看到系统帮助。**

输入：

setup

此时会启动设置菜单，如下所示：

```
                    APN GW CONFIG

AUTHCYBER.COM APN GW1 CONFIG
  Copyright (C) 2001-2016, All right reserved
You should read the INSTALL MANUAL first,  Enter: setup for this
If you are first time to config it on the step 1,2,3,4
The APN GW configuration choices are:
1 - APN GW LICENSE   (VDOMAIN/VHOST/LICENCE/VPUBKEY)
2 - APN LAN NETWORK (LAN IP/MASK)
3 -  WAN  LINK            (ADSL/DDN/ISDN/Dial-up)
4 - SAVE RUN_CONFIG TO START_UP_CONFIG
0 - EXIT CONFIGURATION:  Exit to system prompt.
Your  choice?
```

对于新机，应按照 1，2，3，4 **的次序来进行系统配置。其中各项的作用：**

1. APN Licenses**：有** VDOMAIN，VHOST **及** VDOMAIN **及** VHOST **对应用的** Licenses **项组成。要互相通讯的结点之间用共同的** VDOMAIN **项，相同的** VDOMAIN **结点之间的** VHOST **不能重用，即同** VDOMAIN **之中，每个结点都要有不同的** VHOST，Licenses **是一个** 16 **位或** 24 **位的** ASCII **字符，其包装中会有提供。每个** APN GW **机都要其唯一的** License。**由** APN GW **提供商提供。**

   配置内容：

   Every APN GW have a unique VDOMAIN/VHOST License

       APN GW at the same VDOMAIN and Authenticate PSK

       can communication to each other.

   APN GW VDOMAIN(Default:unkonw): ***your domain***

   APN GW VHOST(Default: unknow): ***your host***

   APN GW LICENCE (Default: APNLICECESNUST24BYTES):***your license***

   Authenticate PSK(Default: public):***pre-share Key***

   ** Summary of what you entered **

   AUTHBY = Pre-share-key

   APN GW VDOMAIN : demo

   APN GW VHOST : demohost

   LICENCES : WrWtg4gk6O8rPowd7qqn4j

   Authenticate PSK : public

Accept these settings and adjust configuration files (y/n)? ***y***

APNGW **要能够通过** IKE **方式协商密钥，必须具有以下两个条件：两端配置有匹配的** POLICY**；两端配有匹配的安全策略（此安全策略当然不用配置验证与加密密钥）。在** POLICY **中用户事先定义了一些** IKE **协商的自保护措施，他们包括：协商报文的加密算法，验证方法，散列算法，使用的** DH **组标识，安全连接的生存时间等等。验证方法的定义非常重要，我们以** pre-share **这种验证方法为例，这是一种秘密密钥验证方法。**

2. APN Network**：局域网设置，用于设定** APN GW **的局域网口参数，现在的** APN GW **提供的是** 100Base-T Ethernet **接口。配置** APN GW **的** IP **地址及其子网掩码。局域** IP **地址可为任何有效的** IP **地址，但建议使用保留的** IP **地址段：**

   A **类地址：**10.0.0.0 ~ 10.255.255.255.0
   B **类地址：**172.16.0.0~172.31.0.0
   C **类地址：**192.168.0.0 ~ 192.168.255.255

注意：因为 172.31.250.0 ~ 172.31.250.255 **作为** APN GW **外网网卡的保留的初始地址，故这段网络的地址也不要使用。**

注意：同 VDOMAN 的每个结点的网络地址不能重复，否则会导致相同网络地址的结点不能与其它任何结点进行通讯，也不能上 Internet **网络。**

配置内容：

APN GW IP Address
Enter the IP address of the Internal network
(default 192.168.0.63): **192.168.250.10**

APN GW IP Address Netmask
Enter the IP Netmask of connected to the internal network
(default 255.255.255.0): **255.255.255.0**

** Summary of what you entered **
APN GW IP Address: 192.168.250.10
Netmask: 255.255.255.0

Accept these settings and adjust configuration files (y/n)? ***y***

3. WAN LINK**：是配置广域联接的选项。支持的广域联接接口有：外置** 56K Modem **拨号，**ISDN TA **拨号，**ADSL **的** PPPoE **接口，及** DDN, Ethernet **接口。进入本项后。会要求输入广域联接方式，四个接网方式在任一时刻只能用其中的一种方法上网，当配好一种方式上网后别的方式自动失效。**

```
APN WAN: Select the way to link to Internet

1 - Dialup      : Use Extend Modem Link to Internet
2 - ISDN        : Use ISDN TA Link to Internet Must a extend device
3 - ADSL        : ADSL Link to Internet
4 - DDN/FIX IP  : DDN or other lease line link to Internet have fix ip
0 - EXIT TO Main: Return to main menu

Your choice?
```

选取 ***1*** —Dialup，**进行拨号上网方式的有关配置。**

配置内容：

Enter the phone number of your ISP
Phone Number: ***163***
Enter your dial-up username
Username: ***163uid***
Enter your dial-up Password
Password : ***163passwd***
** Summary of what you entered **
Dial Up Number : 163
Dial Username : 163uid
Dial Password : 163passwd
Accept these settings and adjust configuration files (y/n)? ***y***

注意：上面文件中如下的内容是用户输入内容。是拨号的对端电话号码及分配的帐号。对于是通过分机上网的，要在被拨的电话号码前加，拨外线的号码及一个"，"号。如拨外线的号为'9"，**拨** 163 **的电话可以拨：**"9,163"。

选取 2 —ISDN ，**与** ISDN TA **进行互联的方式。**

同 1。

选取 3 —ADSL，**与** ADSL Cable Modem **进行联接的方式。**

Enter your PPPoE user name
Username: (default uid@163.gd): your_username@163.gd

Enter your ADSL Password
Password：password

** Summary of what you entered **
PPPoE User name：your_username@163.gd
Password : passwdhere

Accept these settings and adjust configuration files (y/n)?y

选取 4 —DDN，**通过** Ethernet **的联接方式。**

系统接线为：APN GW **的标有** ADSL/DDN **字样的接口通过标准交叉双绞线** Route **的局域网联接，或是通过以太网接入可上互联网的** HUB。**此接口与** ADSL **接口共用一个物理** RJ45 **接口。**

配置内容：

DDN IP Address
Enter the IP address of the Internal network

(default 172.168.250.250): **202.104.177.177**

APN GW IP Address Netmask
Enter the IP Netmask of connected to the internal network
(default 255.255.255.0): **255.255.255.240**

** Summary of what you entered **
DDN IP Address: **202.104.177.177**
Netmask: **255.255.255.240**

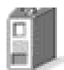
Accept these settings and adjust configuration files (y/n)? ***y***

4. Save Run_Config to Start_up_Config

您做了设置之后，运行无误后，别忘了选择此项存入 APN。**如果您没有选择此项功能，那末您的本次的设置在启动时将丢失。**

注意： APN **系统运行时，所有的程序运行于随机存储器之中。您做的设置只是对当前的操作有效。如果您需要把当前正确的设置保存下来，您一定不要忘记选择此项存于** APN **系统中。否则系统启动后会自动恢复到上一次存取的状态。**

设置步骤小结



如果您是首次使用 APN，**下面的小结可能让您在** 5 **分钟内学会使用。我们以设置** ADSL **虚拟拨号上网为例。**

第一步 用 root **作为用户名，**gw1admin **作为初始密码进入系统，键入** setup；
第二步 选择 1，**按《最终用户许可协议》上所示内容输入** vdomain，vhost **和** licenses；
第三步 选择 2，**设置连接内部网络的** eth0 **接口卡的** IP **地址和子网掩码；**
第四步 选择 3，**再选择** ADSL，**输入用户名和密码；**
第五步 选择 4，**保存以上设置；**
第六步 重新启动 APN（**直接按下电源按钮，然后过两秒后再开**）。**设置完毕。**

高级设置

APN 的配置模式

APN **有三种配置模式。在每个模式里都有相应的命令。下表所列的命令说明了** APN **的所有模式。**

命令模式	功能	系统提示	退出
setup	普通设置模式。登录后能即进入此模式，能执行 setup 设置 APN 的基本参数。	APNGW#	exit

advconf	高级设置模式。在设置模式下输入命令进入此模式。可以设置 APN 的高级参数。	CONF>	exit
fwconf	防火墙设置。可以设置防火墙的策略，对内外网络的管理。	FW>	exit

高级设置支持以下几种配置命令：

APNGW#**help**

Type {apngw|dhcp|telnet|dns|user|pptp|saveall} to config certain function. type exit to quit this mode

APNGW : APN GW Management and multi subnet share configure
DHCP : DHCP Service Configuration and Management
TELNET : Telnet turn on/off
DNS : Domain Name Service Configuration and Management
USER : User Management
PPTP : PPTP Service
CONF>

此时的提示为 CONF>**。在此状态下能支持以上命令。其中：**

APNGW： **用于设置** APN **进程的配置和管理。**
DHCP： **打开或关闭** DHCP **服务。**
TELNET： **用于打开和关闭** Telnet**。**
USER： **用户管理，可以更改用户名、密码、增加用户。**
PPTP： **配置** PPTP **服务端。**
ROUTE： **配置静态路由。**

通用信息：

每个配置都大致有三个公用命令：

start： **开始此项服务；**
stop： **停止此项服务；**
save： **保存当前配置。如果不选择** save **，那么下次启动，当前的配置将全部丢失。**
所以，配置的顺序应该是：

config **或** edit **当前配置**............start（stop）**开始或停止此项服务**..................save **保存配置**

注意： save **存盘时，会把状态一起保存。就是说，如果您配置了某项服务，但是您如果没有启动它的话，那么即使您存盘了下次启动时候还是不会启动。应为它没有把启动或停止的状态保存。**

如何使用 DHCP

APN **系统支持** DHCP**，但该功能在出厂设置时是关闭的。您如果需要使用** DHCP**，您需要在进入** APN **系统设置状态下键入如下命令。**

使用 root **登录，在提示符** APNGW#**下键入：**

APNGW# ***advconf***

系统会提示：

```
APN GW advantage Network Configuration
Type help to list available command.
Type the command to enter certain function menu.
 CONF>
```

输入 dhcp**，可进行** dhcp **的设置。键入** help **可查看所支持的命令。**

CONF> ***dhcp***
DHCP config menu, available command is: {start|stop|config|save}

CONF_dhcp>***help***
Your can use: {start|stop|config|save|exit}

CONF dhcp>***config***
DHCP CONFIGURATION
NETWORK: 192.168.1.1
NETMASK:255.255.255.0

Input your DHCP subnet ip range, first ip address:
(default 192.168.1.0): ***192.168.1.10***

Input your DHCP subnet last ip address:
(default 192.168.1.255): ***192.168.1.200***

CONF_dhcp>***start***
Starting dhcpd:
Address range 192.168.1.10 to 192.168.0.100,netmask 255.255.255.0 spans multiple subnets!
OK.
CONF_dhcp>***save***

通过以上命令，成功配置 dhcp**，其分配地址** 192.168.1.10 **到** 192.168.1.100。

说明： DHCP **支持以下几个命令：**start, stop, config, save, exit。**其含义如下：**
start**：开始** dhcp**，注意此时您应该配置好了** dhcp。
stop**：停止** dhcp**，注意此时您应该配置好了** dhcp。
config**：配置** DHCP。**需要设置** DHCP **开始的地址，中止的地址。**
save**： 把配置文件保存起来。如果您不保存，那么下次启动时会丢失本次配置。**
exit**：退出配置模式。**

如何配置 DNS

APN **可以作为** DNS **服务器使用。但是出厂时，该功能是关闭的。这是从安全角度考虑。一般** DNS **也是** Internet **上容易受到攻击的服务之一。一般情况下，如果您知道当地的** ISP **提供的** DNS**，建议用户**

不要打开本选项。

使用 root 登录，在提示符 APNGW#下键入：

APNGW# ***advconf***

CONF>***dns***

DNS(Domain Name Service)setting, available command is :{start|stip|config|save}

CONF_dns>***config***

You must setting APN License and LAN IP address before build DNS!

(您需要先配置 APN 的 Licenses 和内部网络接口的 IP 地址)

配置之后，用 start 激活，再用 save 保存，DNS 就配好了。如果您配置了 DNS，在下一章中的客户端设置中，您就不需要知道 ISP 的 DNS 的地址了。只需输入 APN 的内部接口的 IP 地址即可。

如何使用 Telnet

APN 系统支持 telnet，但该功能在出厂设置时是关闭的。您如果需要使用 telnet，您需要在进入 APN 系统设置状态下键入如下命令。

使用 root 登录，在提示符 APNGW#下键入：

APNGW# ***advconf***

CONF>***telnet***

TELNET config menu, available command is {start|stop|save}

CONF_telnet>***start***

THIS WILL ALLOW ROOT TO LOGIN APN GW VIA PRIVATE NETWORK OR INTERNET.

OPEN THIS SERVICE MAY CAUSE SERIOUS SECURITY PROBLEM. BE SURE CHANGE ROOT PASSWD AND SAVE IT BEFORE YOU USE THIS FUNCTION.

Note:

use: advconf user passwd, advconf user save, to change root password.

Be sure to open telnet service (y/n)? ***y***

Starting inetd: OK

CONF_telnet>***save***

说明： telnet 支持以下几个命令：start, stop, save, exit。其含义如下：

start：打开 telnet 功能；

stop：关闭 telnet 功能；

save： 把配置保存起来。如果您不保存，那么下次启动时会丢失本次配置。

exit：退出配置模式。



警告：打开 telnet 可能会存在安全隐患。如果打开，您切记要更改 root 的密码。

在出厂设置中，telnet 是关闭的。如果您一旦打开，就可以通过远程登录到 APN 对其进行设置。所以，您一旦打开该功能，需要更改 root 及其密码以确保 APN 系统的安全。

如何配置 PPTP 服务端

APN 可以启动 PPTP 服务。

CONF> ***pptp***

PPTP Management

Available command: {adduser <uid>|deluser <uid>| listuser | start|stop|save|exit}

其中

adduser **用于增加一个用户；**

deluser **用于删除一个用户；**

listuser **用于显示当前的用户及其配置；**

start **表示启动** PPTP **服务；**

stop **表示停止** PPTP **服务；**

save **表示把现在的设置存盘。**

CONF_pptp> ***adduser***

PPTP New user's username: ***olym***

Password for PPTP user <olym>: ***newpass***

CONF_pptp> ***listuser***

User Server Passwd IPnumber

----

olym * newpass *

注意：在配置 PPTP **之后，您需要先** start **此项服务之后，再** save**。因为** save **不光是保存了您的配置，还把您是否启动该项服务的状态也保存了下来。**



诀窍：

您可以一次键入命令完成最终的具体设置模式的命令。

例如：您需要配置 telnet**，您可以使用：**

APNGW#***advconf telnet start*** **启动** telnet



诀窍：

在 CONF>**模式下，或在具体应用设置模式下，您可以使用** help **来查看所有支持的命令。例如**

CONF_telnet>***help***

You can use:{start|stop|save|exit}

如何增加静态路由

APN **可以手工增加静态路由。**

CONF> ***route***

static Route Setting, available command is: {edit|list|start|stop|save}

CONF_route>***edit***

进入编辑界面，可以输入路由规则。

route add –net 192.168.88.0 netmask 255.255.255.0 gw 192.168.0.254 metric 1 dev eth0

说明： 这里是把到 192.168.88.0/24 **这个网段的包通过** 192.168.0.254 **这个网关出去。一般来说都是在本地局域网的。**Eth0 **是本地** Lan **的接口。**

配置完毕，用 ctrl＋w **存盘，**ctrl＋c **退出。**

CONF_route> ***start*** ＃**启动设置**

CONF_route> ***stop*** ＃**停止设置 （可能需要重新启动** APNGW**。）**

You must restart APN GW to reset route table

CONF_route> ***save*** ＃**保存设置。包括是否启动的状态也保存下来。**

安全设置

APN 的安全设置

APN **支持多种加密算法。**

命令模式	功能	系统提示
ipsec config	设置通讯的加密算法。	APNGW#
ipsec auto status	查看 IPSec 的状态。	APNGW#

[APNGW /]# ***ipsec config***

```
 Available ESP Encrypt
No.      Name            Speed  Comp.     Full_Name
-------------------------------------------------
1        null            89        NULL
2        aes             55        AES/128
3        3des            35        3DES/168
4        serpent         57        SERPENT/128
5        blowfish        63        BLOWFISH/128
6        twofish         62        TWOFISH/128
7        sjwa            80        SJW16A
-------------------------------------------------
 Available Authentic
 No.     Name            Speed  Comp.     Full_Name
-------------------------------------------------
1        md5             56        MD5-96
2        sha1            44        SHA1-96
3        sha2_256        42        SHA2-256
4        sha2_512        31        SHA2-512
-------------------------------------------------
esp encrypt(Default: blowfish):aes
auth type(Default: md5):md5
apn: no process killed
Now you have new encrypt way: blowfish-md5, You must restart APN GW or
Restart apngw by : advconf apngw restart, to take it to work.
```

其中的数值，表示速度的参考。这是我们在标准的 100M **的网络环境中用低端设备（处理器为** cy233，64Mram**）的测试值。以** NULL **为基数，其他的加密算法对速度的影响可参考该值。**

其中的 sjwa **是指** SJW16 **硬件加密卡。需要在** GW2500 **型号中支持。**

进行加密算法选择之后，您需要运行 ***advconf apngw restart*** **或重新启动机器来重新建立** VPN **隧道。**

查看当前的 IPSec 信息

[APNGW /]# ***ipsec auto status***

ipsec auto: warning: obsolete command syntax used

000 interface ipsec0/ppp0 218.17.70.18

….

"jklspace.superman_jklspace.gw4":

176.16.10.0/24===218.17.70.18[@jklspace.superman]---218.17.65.

1...218.17.3.1---218.17.3.228[@jklspace.gw4]===192.168.138.0/24

000 "jklspace.superman_jklspace.gw4": ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s; rek

ey_fuzz: 100%; keyingtries: 1000 "jklspace.superman_jklspace.gw4": policy: PSK+ENCRYPT+TUNNEL+PFS+DISABLEARRIVALCHECK; interface: ppp0; erouted

000 "jklspace.superman_jklspace.gw4": newest ISAKMP SA: #8; newest IPsec SA: #2; eroute owner: #2

000 "jklspace.superman_jklspace.gw4": ESP algorithms wanted: 7/000-1/000,

000 "jklspace.superman_jklspace.gw4": ESP algorithms loaded: 7/128-1/128,

000

000 #8: "jklspace.superman_jklspace.gw4" STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2042s; newest ISAKMP

000 #2: "jklspace.superman_jklspace.gw4" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 10780s; newest IPSEC; eroute owner

000 #2: "jklspace.superman_jklspace.gw4" esp.ab6221d@218.17.3.228 esp.4d49128e@218.17.70.18 tun.1002@218.17.3.228 tun.1001@218.17.70.18

000 #7: "jklspace.superman_jklspace.gw4" STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_EXPIRE in 236s

这里可以看到 IPSec **建立的顺序，**IKE **的信息，例如加密算法，密码更新时间等。**

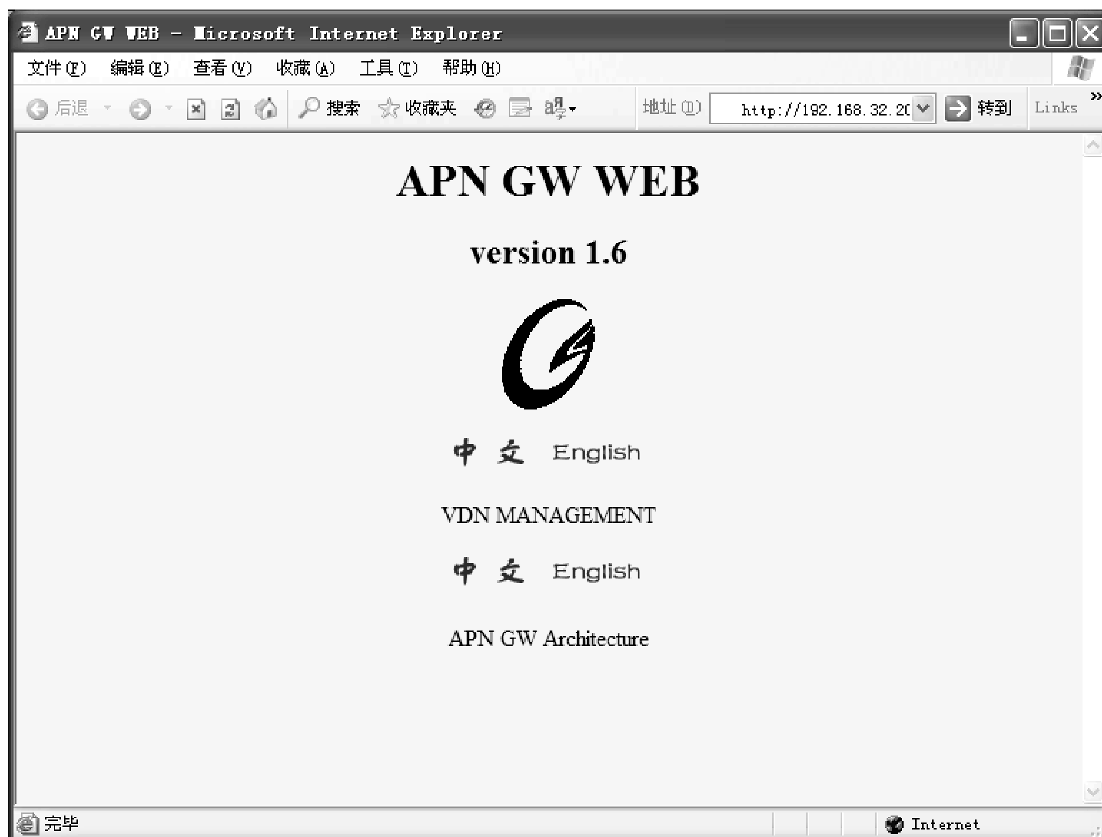
第三章　使用 Web 方式配置 APN

可以直接使用浏览器（推荐使用 Microsoft IE5.0 以上版本 ）配置 APN。用浏览器可以比较直观的配置 APN GW 的绝大多数参数。

如果您的电脑连接到防火墙的局域网接口，您可以在浏览器中输入以下内容：

http://192.168.32.200/

注意：配置之前，必须让您的电脑与 APN 在同一个网段。即您应该配置您的电脑的 IP 地址为 192.168.32.X，子网掩码为 255.255.255.0。



此处可以有两个主要的设置。一个是设置 APN GW5000 的 VPN 通讯网关功能的设置，另外一个是作为 VDN 服务的设置。



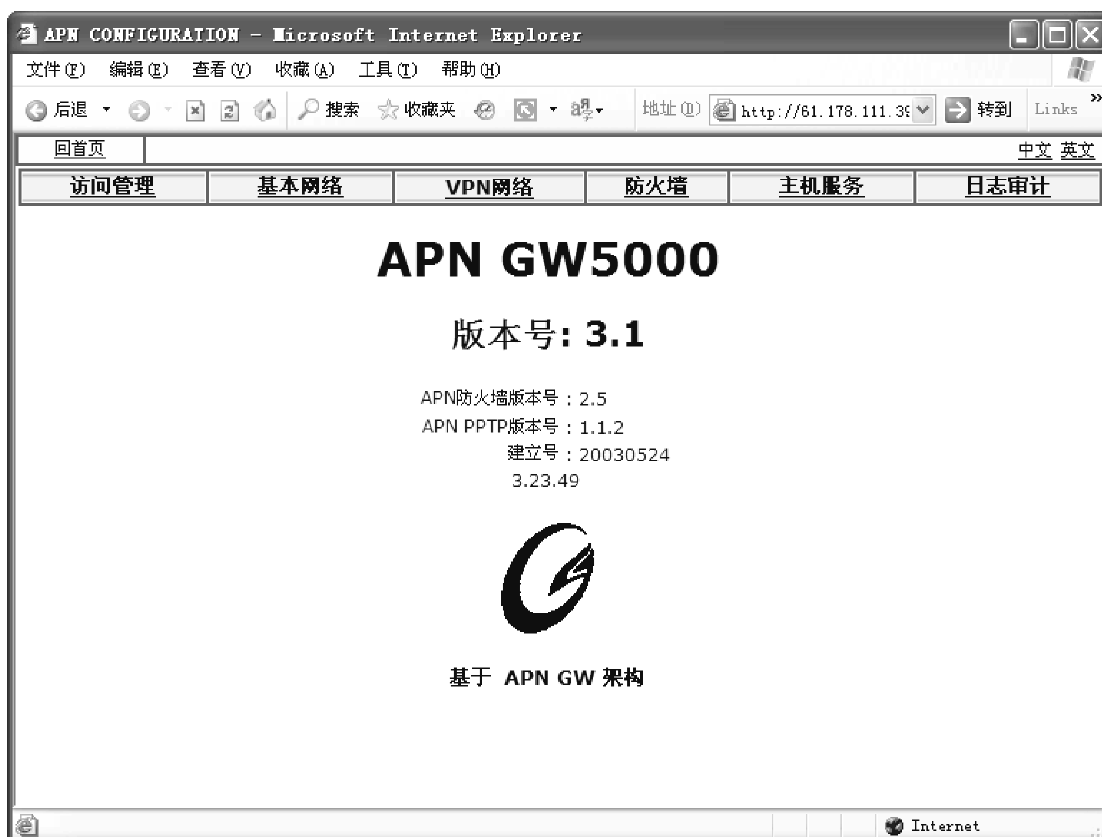
第一个连接是作为 VPN 通讯网关的配置。第二个连接是作为 VDN 服务系统的配置。

VPN 通讯网关的设置

基本配置

您可以选择中文或英文来配置 APN。进入主配置界面。

此处输入用户名 ***root*** ，缺省密码是 ***gw1admin***。先进入作为 VPN 通讯网关的设置。

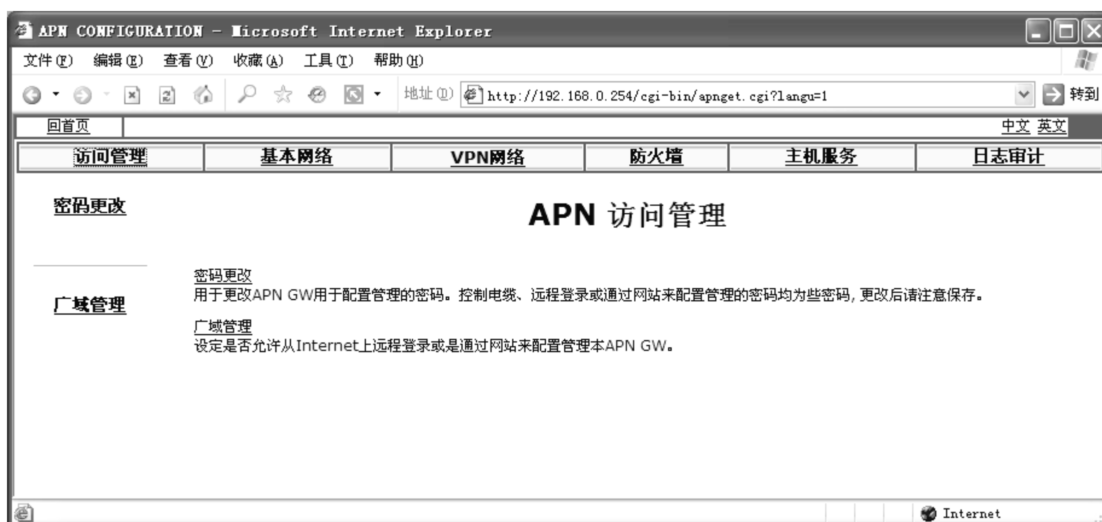


可以看到有以下配置内容：

- 访问管理：主要配置是否可以打开外网接口，以便可以从外网上来管理防火墙；以及系统登录的用户名和密码；
- 基本网络：用于设置防火墙的以太网地址、广域网连接方式、DMZ 接口的信息。
- VPN 网络：用于设置建立 VPN 时候所采用的加密算法、验证方式等。
- 防火墙：用于配置防火墙策略。NAT/DMZ 等。
- 主机服务：用于设置防火墙的主机服务。例如 DHCP、DNS 等。
- 日志审计：用于查看系统日志或配置日志的存储位置。

打开外网访问许可

选择 "访问管理 "



选择广域管理，把"允许从广域网访问本机"激活。（出厂是关闭的）这样可以通过外网或 DMZ 访问本机。注意！：一般情况下，不要打开。除非您需要从远程对 APN 进行配置。



提交之后，您可以从外网（例如 Internet 访问和配置 APN)。

本项配置之目的，在于给 APN 加一个外网访问的开关。缺省设置为关闭，您如需要远程调试，可以把它启用。如果您的配置已经完毕，建议您关闭此选项，它不会影响 VPN 隧道的通讯。

更改登录密码

首先您可以更改系统登录的密码。系统缺省的用户名是 root。密码出厂设置为 gw1admin。



这里您需要输入原来的密码，做输入新密码和确认新密码。设置时候系统会自动检测以下情况：

1. 新密码和旧密码十分相似，将被拒绝；例如原来密码为 gw1admin 您改为 gw2admin ；
2. 新密码过于简单，例如 1111111，将被拒绝。

那些字典里的单词、或者全是大写或全是小写的以及没有包含数字或特殊字符的字符串是不能用来做密码的。建议用下面的规则选择有效的密码：

1. 密码至少要有 6 个字符，最好包含一个以上的数字或特殊字符。
2. 密码不能太简单，所谓的简单就是很容易猜出来，也就是用自己的名字，电话号码、生日、职业或者其它个人信息作为密码。
3. 密码必须是有有效期的，在一段时间之后就要更换口令。
4. 密码在这种情况下必须作废或者重新设定：如果发现有人试图猜测你的密码，而且已经试过很多次了。

设置网络参数

选择基本网络



可以设置

局域网 IP**：设置本机与局域网相连的** IP **地址。**

DMZ IP**：设置** DMZ **区的** IP **地址。**(**部分型号**)

广域网连接方式：设置广域网连接的方式。例如固定 IP **地址，或** ADSL **拨号等。**



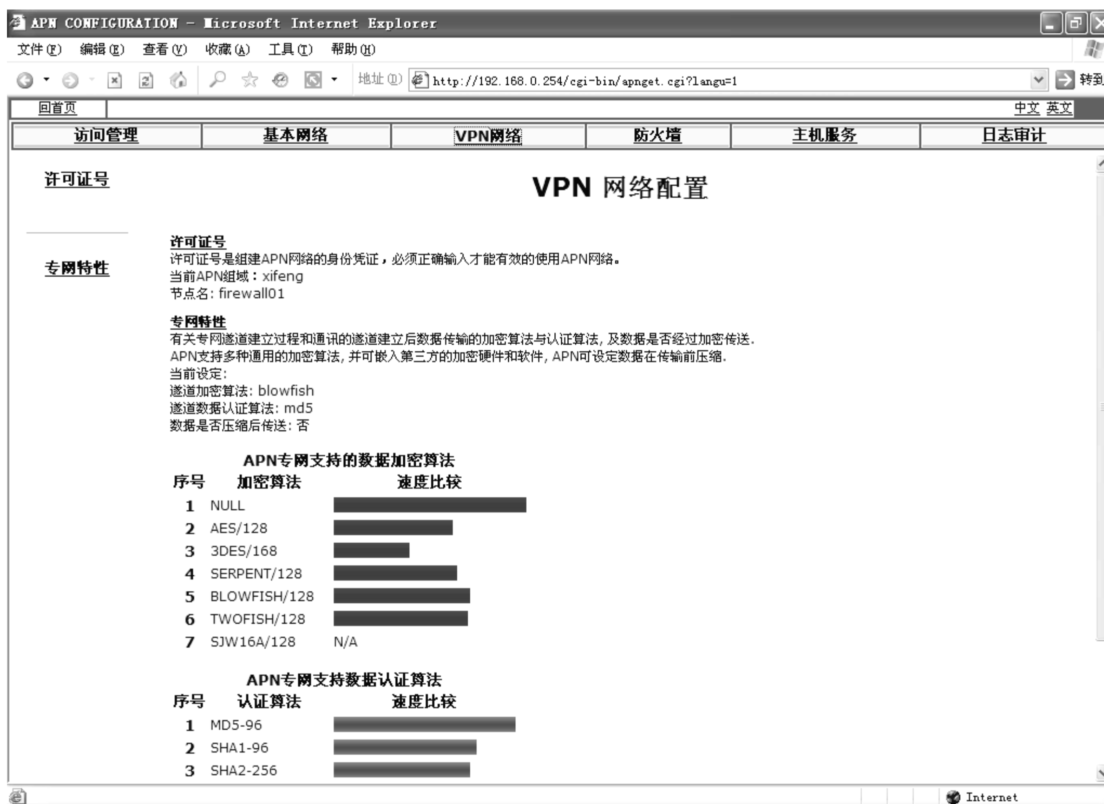


设置了基本的信息，您就可以让 APN 工作了。如果您已经成功完成以上的设置，您就可以在 APN 的防火墙的保护之下，安全的上网了。

VPN 网络设置

APN 的 VPN 网络设置主要设置许可证号、加密方式。

图中可以看到各种加密算法的速度比较参考图。



这里可以设置 VPN 网络的许可证号、以及采用的加密算法等信息。

APN GW 建立 VPN 时候支持

数据传输可自由选择

- AES/128 位加密算法
- 3DES/168 位加密算法
- SERPENT/128 位加密算法
- BLOWFISH/128 位加密算法
- TWOFISH/128 位加密算法
- 硬件加密卡或第三方算法

保证数据完整可自由选择

- MD5-96
- SHA1-96
- SHA2-256
- SHA2-512

身份认证支持

- RSA 2048
- Pre-share Key

APN GW 出厂设置为 BLUEFISH+MD5/96，未启动压缩传送。缺省的 Pre-Share Key 是 public。

注意：出于安全的角度考虑，强烈建议配置时更改 Pre-share Key。但需要保证各节点之间的设置值一致。



APN 支持压缩传输。

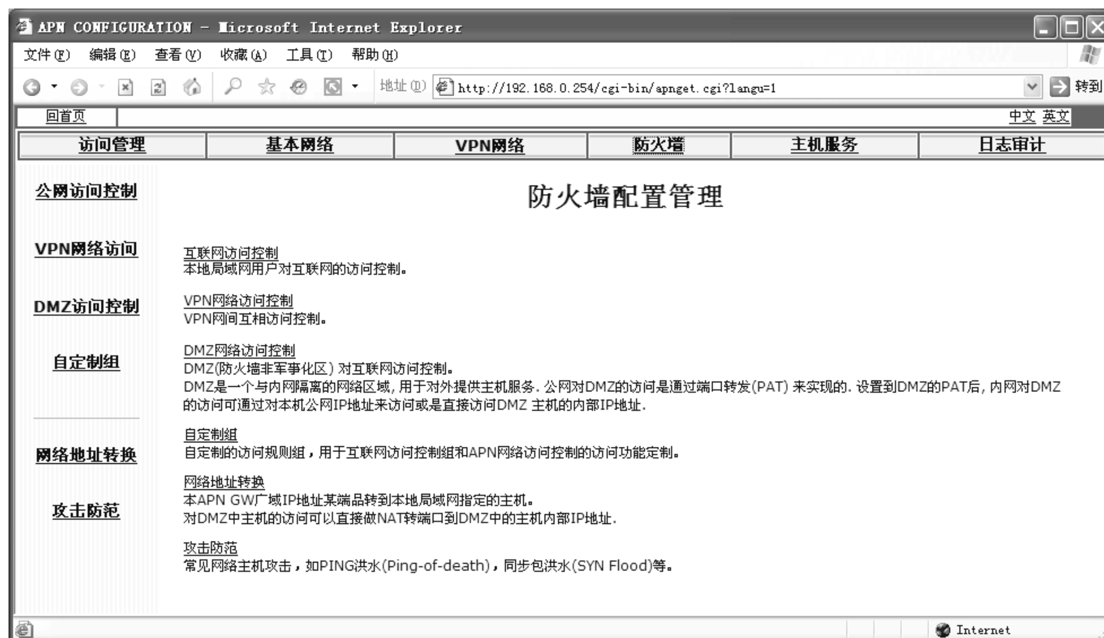
注意：

1． 各节点之间的设置应该统一；

2． 启用压缩后速度不一定因此而提高，这将取决于您的具体应用。一般情况下我们不推荐您启用。

其中许可证号是在 VDN 功能中生成的。在后面的章节中会有描述。

防火墙配置



可以看到以下几个功能：

公网访问控制：设置内网对公网的访问控制。

VPN **网络访问控制：设置** VPN **隧道之内的访问控制。**

DMZ **访问控制：设置** DMZ **区的访问控制。**

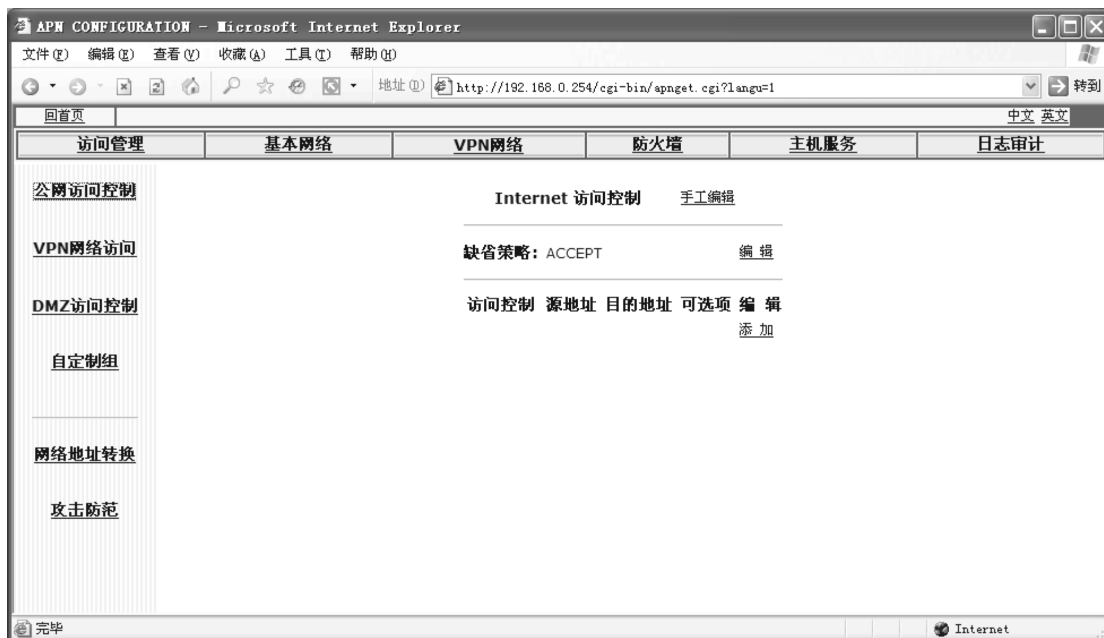
自定制组：设置自己定义组的防火墙策略，可以把这个策略加载在隧道里面和对公网的访问之中；

网络地址转换：设置 NAT **的相关信息。**

攻击防范：内置常见攻击的防范。如 PING **洪水**(Ping-of-death)**，同步包洪水**(SYN Flood)**等。**

公网访问控制

本项设置主要是内部局域网对公网的访问的许可。



设置的思路主要是有两种：

1． 先拒绝所有的；再定制可以接受的；
2． 先接受所有的；再定制需要拒绝的；

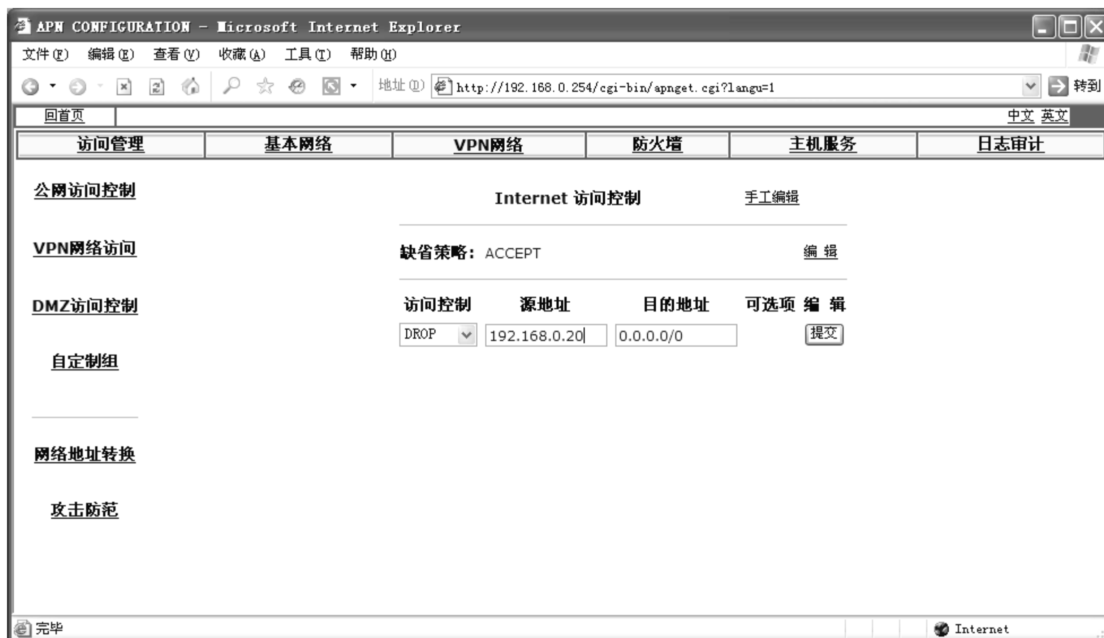
例如：您设置只有 192.168.0.230 这个电脑可以上网，可以先拒绝所有的：缺省策略配置 DROP，然后在访问控制中添加 192.168.0.230 这个地址。

如果您已经定义好了组策略，例如建立了一个叫 DEMO 的组。（其中组的设置参考下一节）这个组有它自己的策略，例如拒绝了 UDP 的 8000 端口。您可以在这个设置界面中看到组的名字，然后可以把您要定制的 IP 地址加入到这个组里面来。

如下图所示：



当然，可以把整个 IP 地址都拒绝掉。



VPN 网络访问控制

本项设置主要是对 VPN 隧道的访问的许可。

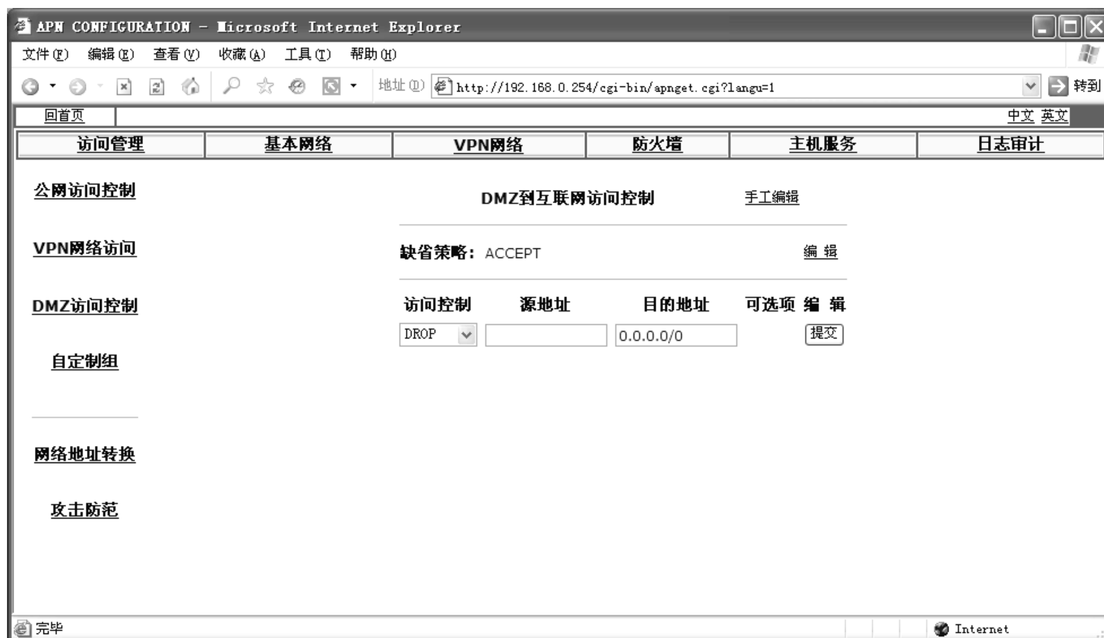
其设置的方法类似于外网设置。也支持组策略，不同的是，其设置的规则只能用在 VPN 隧道之中。



DMZ 访问控制(部分型号)

非军事化区（DMZ）：为了配置管理方便，内网中需要向外提供服务的服务器往往放在一个单独的网段，这个网段便是非军事化区。APN GW 配备三个 10/100M 以太网卡接口，在配置时一般分别分别连接内部网，外部网（Internet）和 DMZ。

DMZ 由于其特殊的位置，黑客从外网即使攻入了 DMZ 区，也进入不了内网。所以一般可以用于用户建立自己的 web 服务、ftp 服务、mail 服务等。而且用户在自己的内部局域网络之内，可以通过外网地址来访问。



这里定义了 DMZ 区对外网的访问许可。

自定制组

APN GW 支持分组管理。

在防火墙设置中，可以定义若干的组。每个组都可以定义多种防火墙策略。例如在一个公司中，可以定义"财务组"、"市场组"、"领导组"，从而规定不同的安全级别和对外网（例如 Internet）的访问权限。然后，可以把某一段 IP 地址或者某一个和多个 IP 地址或者某一个和多个 MAC 地址应用于预先定义好的组中。

定义的组策略，可以应用于对外网的访问或者由 VPN 所建立的隧道之中。

下图示范了定义一个组把 QQ 聊天拒绝了。（UDP 8000 端口）

第一步：建立一个组



第二步：定制组里面的防火墙策略。

选择 DROP，选择协议 UDP，输入端口号 8000，提交之后就建成了。定制完毕之后，您可以自由的选择用于公网访问和 VPN 网络访问之中。

组策略只是定义了策略的规则，没有对某地址或网段作具体的设置。



以下是一些常见的应用的端口号：

http ======> port 80 (Hyper Text Transfer Protocol)

ftp-data ==> port 20 (File Transfer Protocol - Default Data)

ftp =======> port 21 (File Transfer Protocol - Control)

POP3 ======> port 110 (Post Office Protocol version 3)

SMTP ======> port 25 (Simple Mail Transfer Protocol)

OICQ======> UPD 8000

NNTP ======> port 119 (Network News Transfer Protocol)

telnet ====> port 23 (Telnet)

Gopher ====> port 70 (Gopher)

IRC =======> port 194 (Internet Relay Chat)

Proxy =====> port 80/8080/3128 (Proxy)

Socks =====> port 1080 (Socks)

DNS =======> port 53 (Domain Name Server)

hostname ==> port 101 (NIC Host Name Server)

finger ====> port 79 (Finger)

nicname ===> port 43 (Who Is)

login =====> port 49 (Login Host Protocol)

HTTPS =====> port 443 (https MCom)

imap3 =====> port 220 (Interactive Mail Access Protocol v3)

NetBIOS ===> port 137 138 139 (NetBIOS)

NFS =======> port 2049 (Network File Service)

SNMP ======> port 161 (Simple Network Management Protocol)

snmptrap ==> port 162 (SNMP TRAP)

TFTP ======> port 69 (Trivial File Transfer)

更多信息，可以访问我们的 web 站点。

地址转换 NAT

APN GW 都捆绑了网络地址转换（NAT）功能。NAT 使用户能够把专用或非法 IP 地址转换成合法的公共地址。

一般情况下，当用户只有一个 IP 地址时（由 ISP 分配），怎样使几台机器共享一个 internet 连接呢？如果使用不同的源 IP 发出数据包，将只有目的 IP 为拨号机器的数据包才能返回。为了解决这个问题，我们在 APN 内置了网络地址翻译功能，将所有局域网 IP 转换为 APNGW 的 IP，从而实现拨号或其他形式的 Internet 连接共享。这是最常用的一种 NAT。

这被称作"IP 伪装"（IP Masquerading），因为这种情况下数据包的源 IP 被修改，我们称之为"源网络地址翻译"（Source Network Address Translation，SNAT），实际上，更确切的说法是"源 IP 地址翻译"。

有时出于负载均衡或其他原因，我们只有一个 IP，却希望用几台提供服务，这时最好的办法是将几台服务器"藏"在一台拥有合法 IP 的机器，这台机器上启用网络地址翻译，将外来的连接分配至各个服务器，这种情况也被称作"端口转换"，因为这需要在翻译时改变数据包的目的 IP，被称之为"目的网络地址翻译"（Destination Network Address Translation，DNAT）。

APN GW 支持 NAT 和 DNAT。



设置的时候，需要选择协议和端口号，目的 IP 地址。如果您使用的是带有 DMZ 的型号，建议您的服务放置于 DMZ 区之内。

攻击防范

攻击的法律定义是指：攻击仅仅发生在入侵行为完全完成且入侵者已在目标网络内。但是更积极的观点是（尤其是对网络安全管理员来说）：可能使一个网络受到破坏的所有行为都应称为攻击。即从一个入侵者开始在目标机上工作的那个时刻起，攻击就开始了。

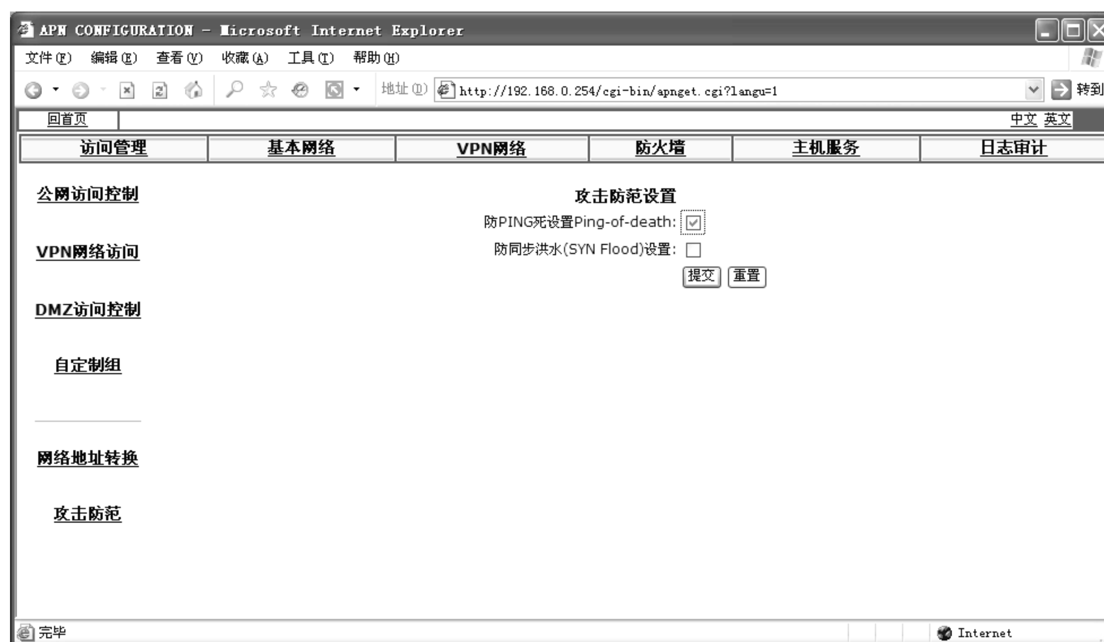
通常，在正式攻击之前，攻击者先进行试探性攻击，目标是获取系统有用的信息，此时包括 ping 扫描，端口扫描，帐户扫描，dns 转换，以及恶性的 ip sniffer（通过技术手段非法获取 ip packet，获得系统的重要信息，来实现对系统的攻击，后面还会详细讲到），特洛依木马程序等。这时的被攻击状态中的网络经常会表现出一些信号，特征，例如：

· 日志中有人企图利用老的 sendmail 就是比较明显的攻击的信息，即有人在端口 25 上发出了两三个命令，这些命令无疑是企图欺骗防火墙将秘码文件的拷贝以邮件的形式发送给入侵者。

· 大量的扫描应立即意识到安全攻击的出现。

· 某主机的一个服务端口上出现拥塞现象，此时应该检查绑定在该端口上的服务类型。淹没式和 denial of service 式的攻击通常是欺骗攻击的先兆（或是一部分）。

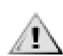
APN 内置的常见的攻击防范。例如 ping 洪水，防止同步包洪水（Sync Flood）。



主机服务

描述了如何定制 APN 的主机服务。包括 telnet、DHCP、DNS 三个服务。

APN GW 提供远程登录、DNS 和 DHCP 服务。

 警告：	如果您打开 telnet 功能，一定请修改初始密码。

提供远程登录服务

您可以以让 APN 提供 Telnet，用于远程的调试。在 telnet 进入系统中，您可以获得更多的配置选择。



一旦选中，提交之后，就启动了 APN 的 telnet 服务。确省情况下，您只是能从局域网中远程登录过去。如果在“访问管理”中打开了公网的访问控制，您可以从公网上登录到防火墙。

提供 DNS 服务

一般情况下，我们并不推荐用户启动 DNS 服务。但是用户在启动 DHCP 配置的情况下，为了设置的方便，可以启动 DNS。直接在页面中提交就可以启动 DNS。



提供 DHCP 服务

APN GW 可以作为 DHCP 服务器。可以为内网的地址提供动态 IP 地址分配。这样可以避免手工设置地址的麻烦。



其中 DNS 可以设置公网上的 DNS，如果您不知道具体的地址，您可以启动 APN 的 DNS 服务，然后该地址就用 APN 的内网地址。

日志查看

主要讲述了如何配置和查看系统日志。

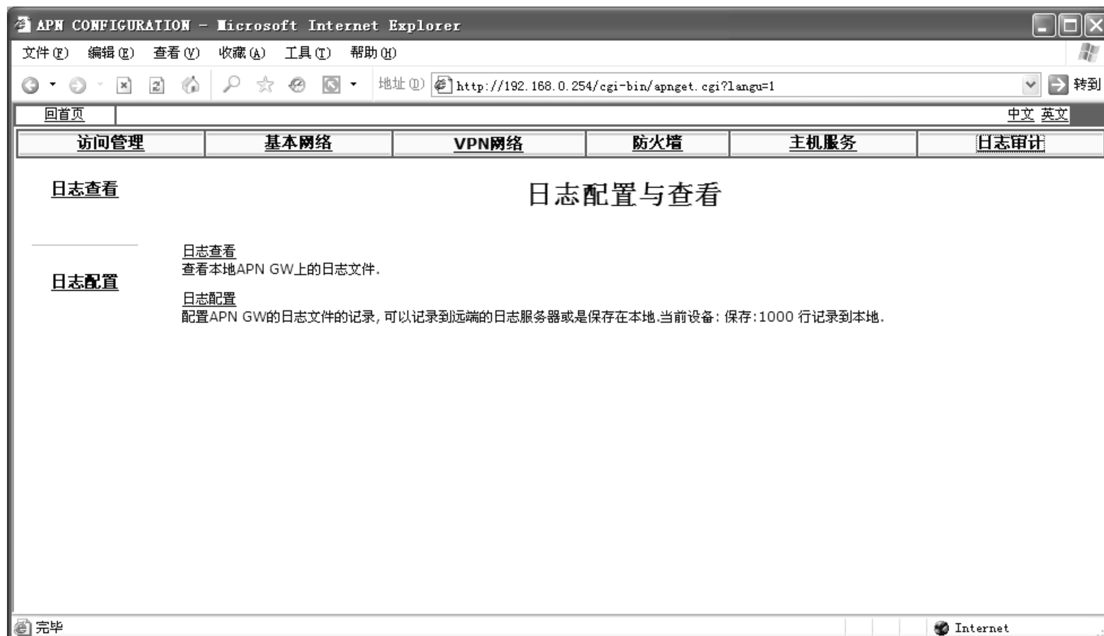
日志概述

日志对于安全来说，非常重要，他记录了系统每天发生的各种各样的事情，你可以通过他来检查错误发生的原因，或者受到攻击时攻击者留下的痕迹。日志主要的功能有：审计和监测。他还可以实时的监测系统状态，监测和追踪侵入者等等。

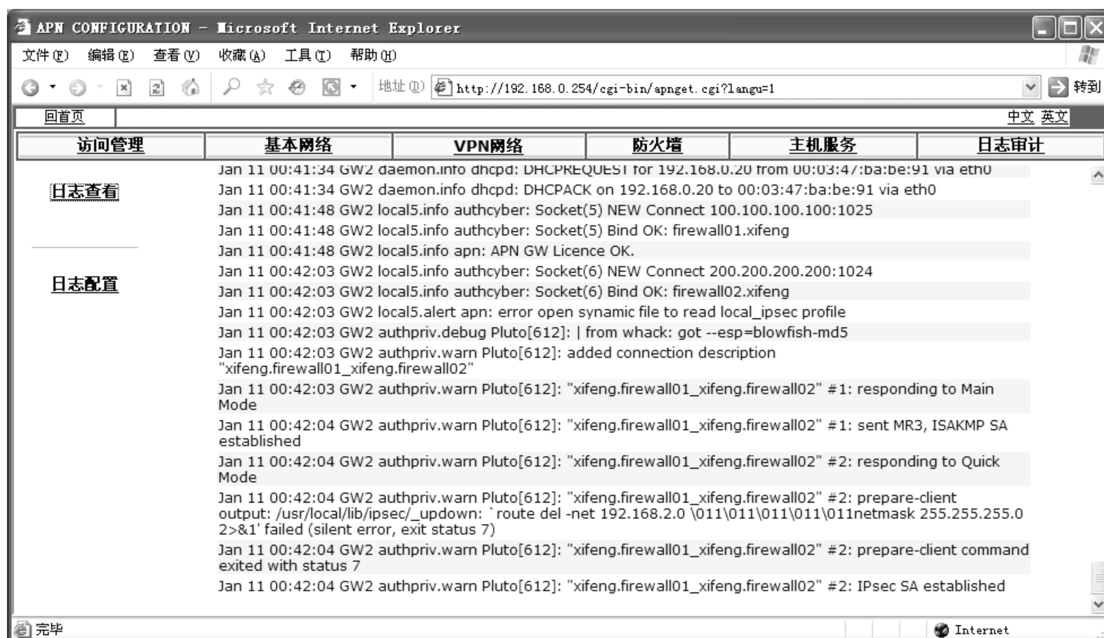
日志文件其实是纯文本的文件，每一行就是一个消息。每一行表示一个消息，而且都由四个域的固定格式组成：

- *时间标签(Timestamp)，表示消息发出的日期和时间。
- *主机名(Hostname)，表示生成消息的计算机的名字。如果只有一台计算机，主机名就可能没有必要了。但是，如果在网络环境中使用 Syslog，那么就可能要把不同主机的消息发送到一台服务器上集中处理。在我们的例子中主机名为 lcbj。
- *生成消息的子系统的名字。可以是 “Kernel ”，表示消息来自内核或者是进程的名字，表示发出消息的程序的名字。在方括号里的是进程的 PID。
- *消息(Message)，即消息的内容。

查看日志



可以在“日志审计”中，看到日志信息和配置日志的存储位置。



配置日志



可以把日志文件存储在本地，也可以存储在远程的专用日志服务器上。

注意：如果存储在本地，最多支持 10，000 行日志。





读解日志

"MARK"消息：在默认情况下每隔 20 分钟就会生成一次表示系统还在正常运行的消息。"MARK"**消息很像经常用来确认远程主机是否还在运行的"心跳信号"**(Heartbeat)。

日志构成：它们是由两个域组成，分别是"选择器(Selector)**"和"动作**(Action)**"。"选择器"用相应的"设备"和"优先级"(都可以用"*"通配符表示"任何一个")来表示消息的类型。"动作"表示一旦有一个新的消息和"选择器"相匹配的时候要采取什么行动。**

每个 syslog **消息被赋予下面的主要设备之一：**

LOG_AUTH--**认证系统：**login、su、getty **等**

LOG_AUTHPRIV--**同** LOG_AUTH**，但只登录到所选择的单个用户可读的文件中**

LOG_CRON--cron **守护进程**

LOG_DAEMON--**其他系统守护进程，如** routed

LOG_KERN--**内核产生的消息**

LOG_SYSLOG--**由** syslogd（8）**产生的内部消息**

Syslog **为每个事件赋予几个不同的优先级：**

LOG_EMERG--**紧急情况**

LOG_ALERT--**应该被立即改正的问题，如系统数据库破坏**

LOG_CRIT--**重要情况，如** IO **错误**

LOG_ERR--**错误**

LOG_WARNING--**警告信息**

LOG_NOTICE--**不是错误情况，但是可能需要处理**

LOG_INFO--**情报信息**

LOG_DEBUG--**包含情报的信息，通常旨在调试一个程序时使用**

例如：

#Sep 11，23：09：53 **这时网卡地址为** 00:00:e2:6f:26:9b **的设备通过内网得到** DHCP **服务分配的地址** 192.168.138.150

Sep 11 23:36:57 GW1 authpriv.info in.telnetd[663]: connect from 192.168.138.248

Sep 11 23:37:00 GW1 auth.info login[664]: root login on `ttyp1' from `192.168.138.248'

#Sep 11，23：37：00 **用户** root **从** 192.168.138.248 **登录。**

VDN 服务系统的配置

回到首页，点击下一个连接，可以进入 VDN 服务配置的界面。



开始配置

在设置之前，对用户和 License（许可证号）的关系做简单描述。

- 每一个用户对应唯一的组域（vdomain）；
- 每个组域中可以有多个节点（vhost）；
- 每一个节点对应一个唯一的 License。

建立一个新的许可证的步骤如下：

- 建立一个新用户，输入用户的详细的资料。
- 建立一个新的组域；
- 在该组域中建立新的节点；

如果是第一次配置 5000，先添加一个用户。选择用户管理－>新加可以增加用户。

用户管理

点击用户管理。可以进入用户管理页面。此处可以查看用户、查找用户和增加新用户。



点击新加用户，可以输入用户的信息。用户信息包括客户的公司名称、联系人等。需要详细的输入以便于以后的维护。



点击查看，可以看到目前数据库中所有的用户信息。



点击查找，可以通过模糊查询查找所有的相关的信息。

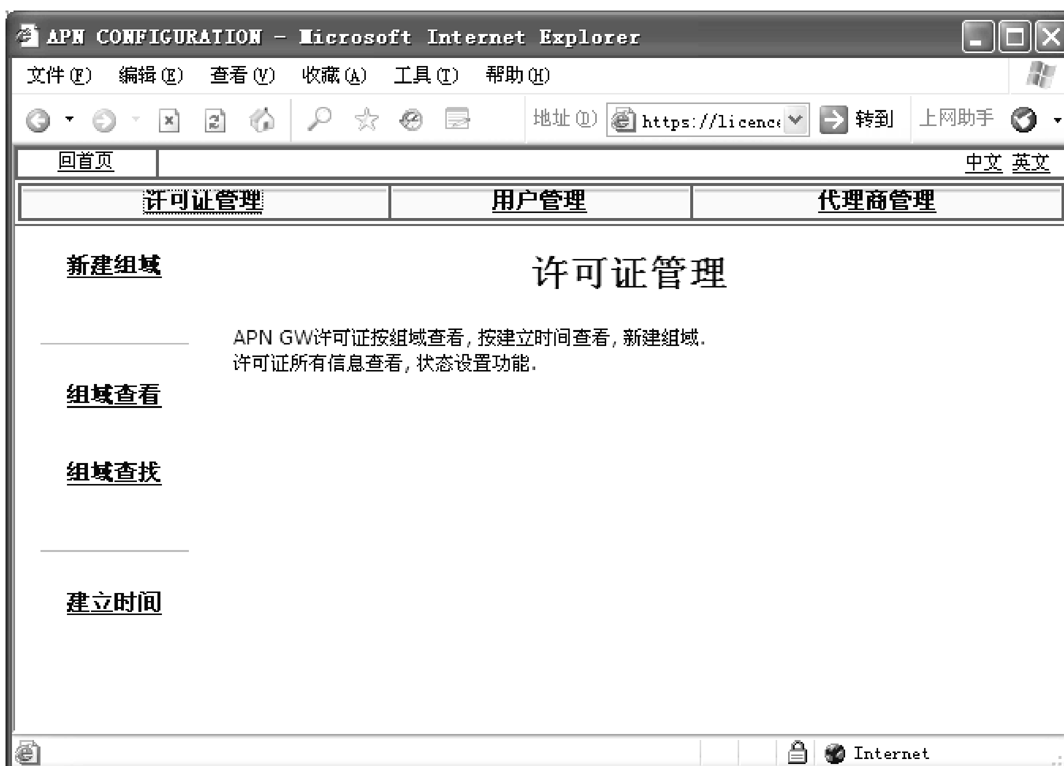
此处可用通过输入汉字来查询。只有用户的名称中含有该汉字，就可以查询出来。例如：



提交后，可以查询所有含有输入字样的信息。



许可证管理



许可证管理分为新建组域、查看、查找以及按照时间查找。

点新建组域，可以建立一个新的 vdomain。**标准的** 5000，**只能支持** 1 **个域。**



其中组域号只能用英文字母，最少不得少于 3 个字母。节点名也是英文字母，最好能与节点所在地理位置上对应。同时可以一次性建立多个 License。如果是多个将在 vhost 后面递增的加入 001、002、003 类推。同时该域对应于某一个固定的用户。如果这时候是对已经存在的用户发放 License，同时可以新建一个用户。关于用户的建立和管理，可以参考下一给节的设置。

点组域查看，可以看到所有的 License 的情况。包括节点数目、终端型号、通讯端口、代理商名称、用户名称等信息。点击其中代理商名称或 vdomain，可以看到相应的细节。



如果客户需要增加 License，而管理者又忘记其初始的 vhost 等信息的情况下，可以点组域查找，查找原来的 license。



此处可以输入组域进行模糊查找。例如：

原来的的 vdomain 中有 abcdef、rbcd、bcd、bcdf、fbcd 者几个 vdomain，可以通过输入 bcd 把以上所有的域查询出来。例如：



组域	节点数	类型	服务端口	代理商	用户
novadg12	2	1	6101	olymtech	东莞南凌
novagw1	2	1	6101	olymtech	东莞南凌
novagw11	2	1	6101	nova	南凌科技
novanew005	2	1	6101	olymtech	奥联科技
dgnova	4	2	8401	nova	南凌科技
novanew01	4	2	8401	nova	南凌科技
novanew02	3	2	8401	nova	南凌科技
novanew03	2	2	8401	nova	南凌科技
novanew1	2	2	8401	nova	南凌科技
novasz01	2	2	8401	nova	南凌科技
合计: 10	25				

以上页面是查询 nova 的信息所显示的关于 nova 的所有信息。其中点击域可以查看该域的所有的 vhost 和 license，同时可以在增加新的 license。点击用户可以查看每个用户的详细情况。

有时候，可能需要按照时间来查看，点击建立时间，可以看到按照时间排序的信息。



冻结和删除 license

在上面的用户查找和组域查找中，都可以点击相应的信息。



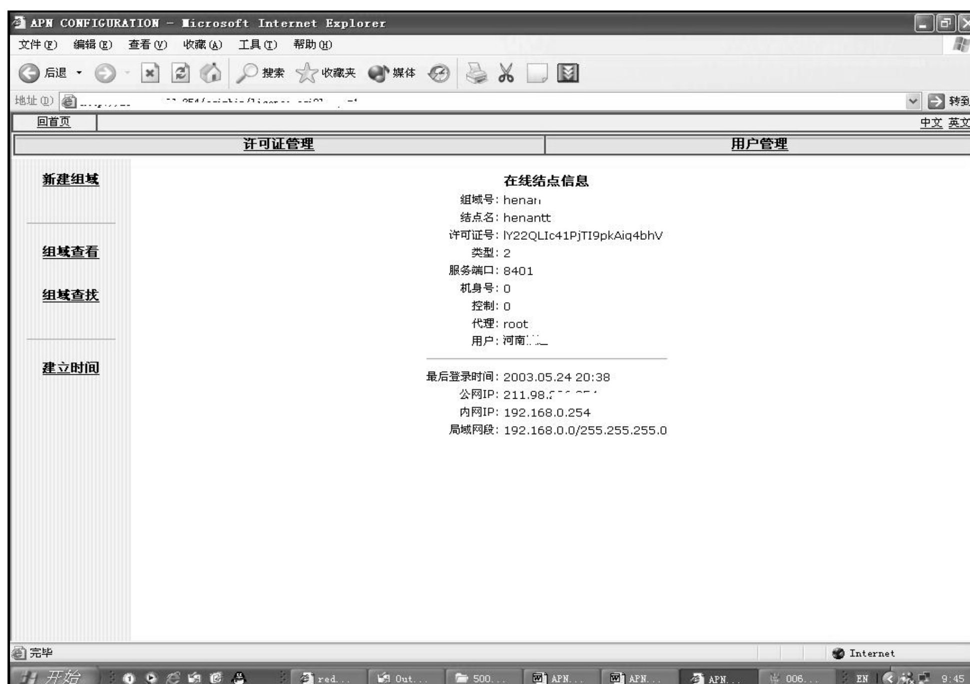
点击 Edit，



此处可以删除 License，同时，还可以输入机器号码以便于以后维护。如果在“控制”栏中把 0 变成非 0，则该 License 将会失效。反之，设置为 0 可以恢复。

查看在线节点

进入许可证管理-->组域查看-->组域名-->@，进入在线节点信息浏览窗口。



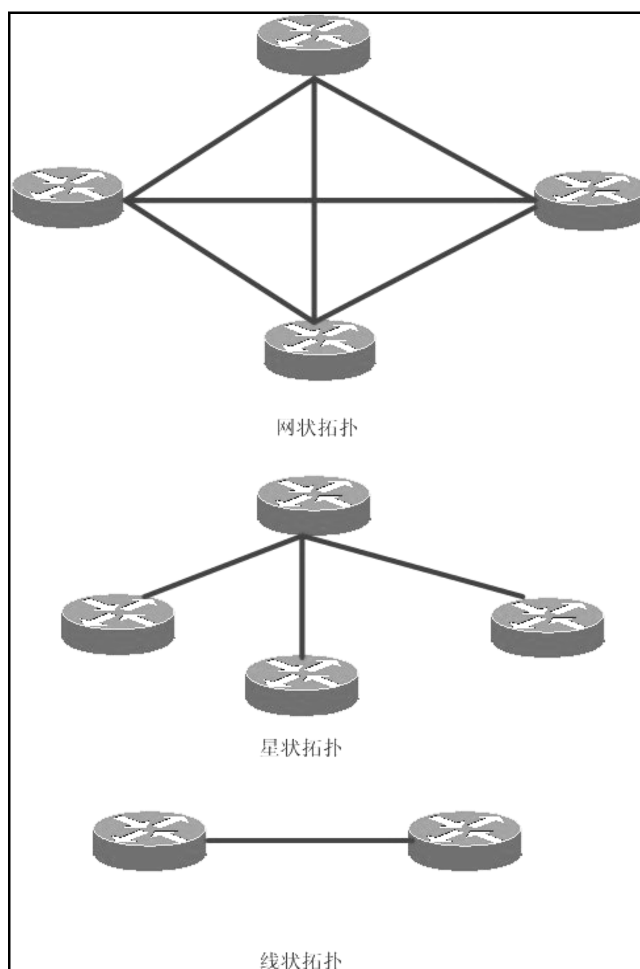
结点可定义特性

对于基于 APN GW 产品的 VPN 解决方案，不同的用户群有不同的网络拓扑要求。如果一个公司总部与分支机构之间都需要交换数据，而且有 IP 电话的应用的话，那么客户要求的网络拓扑是网状。网状的拓扑结构没有中心点，也就没有了瓶颈，各个结点交换数据是独立的，而不需要通过某个中心结点来转发。

如果一个公司所有或者大部分的服务器都是集中在总部机房，其他分支机构之间互相之间不需要直接传输数据。那么客户要求的网络拓扑是星状的，各个分支机构只能跟总部通信。

APN GW 架构提出了三种结构。由这三种结构可以构建不同的任意形状的网络结构。

对于网状、星状和线状拓扑分别如图所示：



结点名定义规则

VDN 结点名分为两部分：VDOMAIN 和 VHOST。VDOMAIN 是由一个字符串组成，可用的字符为字母、数字、下划线。一般取公司名的英文简写或者汉语拼音简写，如果奥联科技有限公司的 vdomain 为：olym。

VHOST 是结点字符串，由字母、数字、下划线组成的字符串与“．”组成。如奥联公司总部的 vhost

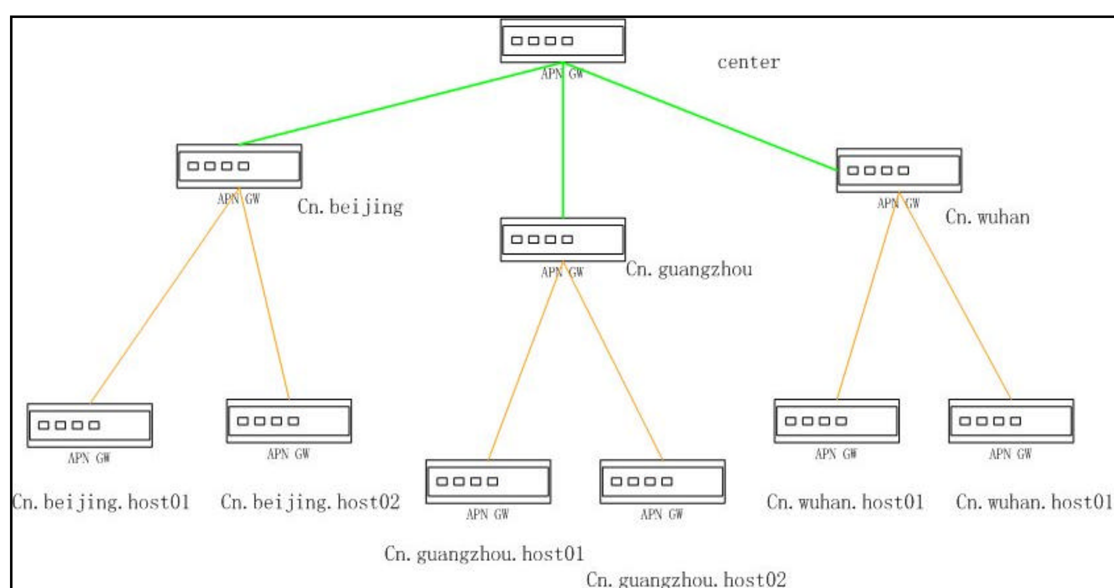
为 center，北京总代理商的 vhost 为 cn.Beijing，北京总代理下面的二级代理商的 vhost 为 cn.Beijing.host01

Vhost 以“．”来划分组和结点，组合结点以最后一个“．”来划分。例如 cn.Beijing.host01，最后一个“．”后面的字符串 host01 为结点， cn.beijing 为组；cn.beijing，beijing 为结点，cn 为组。

定义节点之间的关系

以一个例子来说明如何定义关系：

奥联公司总部在深圳，各个省会城市、直辖市都有总代理和代理商。现在要求所有总代理，代理商结点都跟深圳总部建立隧道，进行数据传输，这可以设计成星形的拓扑结构；第二个要求是各个省的代理商之间不允许互相访问；第三个要求是各个省之间的代理商以总代理为中心点，下面的代理商只能跟中心点通信。网络拓扑图如下：



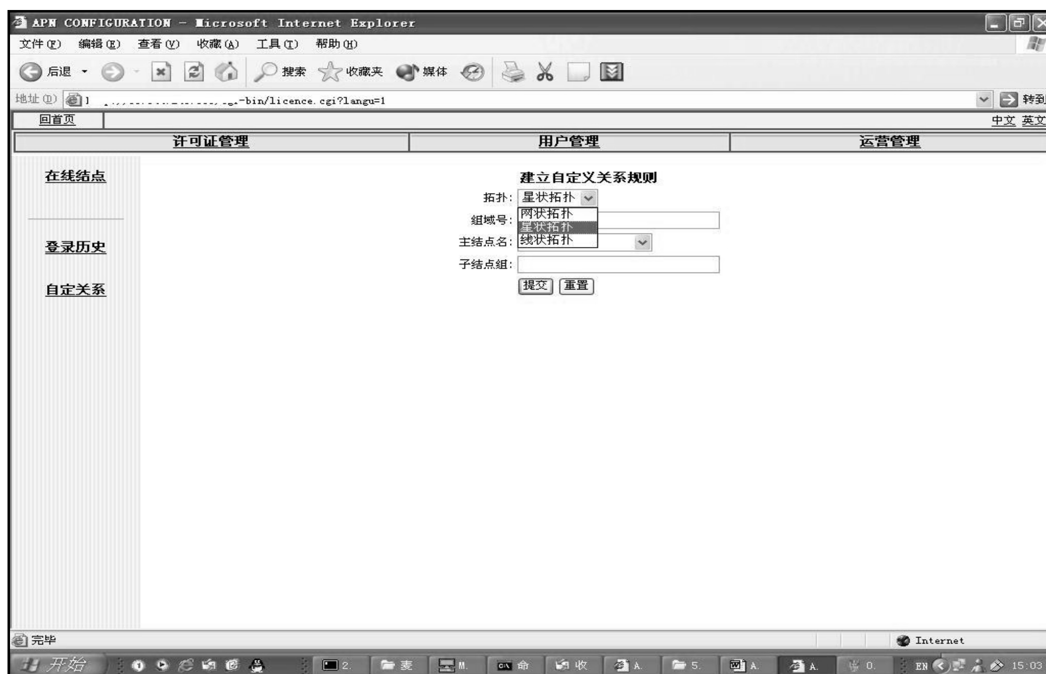
设定步骤：

根据以上的 vhost 发放 licenses；

定义 center 为中心点的星状拓扑；

通过 web 浏览器进入 APN GW5000 web 管理界面；

点击运营管理-->自定关系-->新建，进入新建自定关系界面，如图所示；



拓扑选择星状拓扑，组域号为：olym，主结点名为：center，子结点组为：cn，按提交后，就会在 vdn 数据库里面定义了一条星状的关系。

注意：定义关系的时候，当子结点组为 cn 的时候，包含的结点为 cn.xxxx 的结点，也就是说只包含 cn 为组名，xxxx 为结点名的结点。如上面包含的结点是：cn.Beijing、cn.guangzhou、cn.wuhan，而不包含 cn.Beijing.host01 等。

定义 cn.beijing 为中心点的星状拓扑；

新建一个自定义关系，拓扑选择星状拓扑，组域号为：olym，主结点名为：cn.beijing，子结点组为：cn.beijing，按提交后，就会在 vdn 数据库里面定义了一条星状的关系。

根据以上方法定义 cn.guangzhou 为中心点的星状拓扑，cn.wuhan 为中心点的星状拓扑。

保存所有设定：通过 telnet 或者超级终端的方式登陆 5000 界面，在#提示符后输入 dbsave 命令保存所有设定。要注意的是，刚才所有的配置都只保存在内存的虚拟空间里面，要想再次启动设备配置生效，在修改和增加配置后，必须运行 dbsave 命令。

假设奥联总部跟总代理之间的拓扑是网状的连接，只需要将刚才配置的第一条自定义关系的拓扑改为网状拓扑就可以了。

计算新的 cache 值

cache 值的概念：APN GW 通讯网关设备是通过设置的 cache 值来找到 5000 的 VDN 服务的，cache 值是通过 5000 的公网 IP 地址计算出来。

如果修改了 5000 的公网 IP 地址，需要重新计算 cache 值，并且修改 5000 以及其他节点的 cache 值，注意修改后请重新启动机器。

使用 console 线或者 telnet 方式进入 5000 终端管理界面，在#后输入命令：

#[APN GW]***conv*** 新的公网 IP 地址，如#conv 202.96.134.133，记录计算出来的新的 cache 值，所有需要本 5000 服务的 GW2000/2500/5000 等设备，都需要更改 cache 值。通过 console 或 telnet 进入设置界面，输入：#[APN GW]***newcache*** 【计算出来的 cache 值】可以更新 cache 值。

第四章 局域网工作站设置

用 APN GW 建立 VPN 通道之后，其所包括的各节点之间的内部局域网可以互通通讯。局域网网内部的电脑（工作站）需要把缺省网关指向 APN 的局域网地址。

设定 TCP/IP **使用其** IP **与** APN GW **在同一个子网中。并且保证不用同一个** IP **地址，以确定不会发生网络冲突。并把** IP **的缺省网关指向** APN GW。

举例说明：如 APN GW **的** IP **地址是：** 192.168.3.10, **子网掩码是**: 255.255.255.0, **那么其它工作站的** IP **可以是：** 192.168.3.1, 192.168.3.2, **或** 192.168.3.11, 192.168.3.12 **等等，但工作站的** IP **不得与** APN GW **的** IP **一样。**

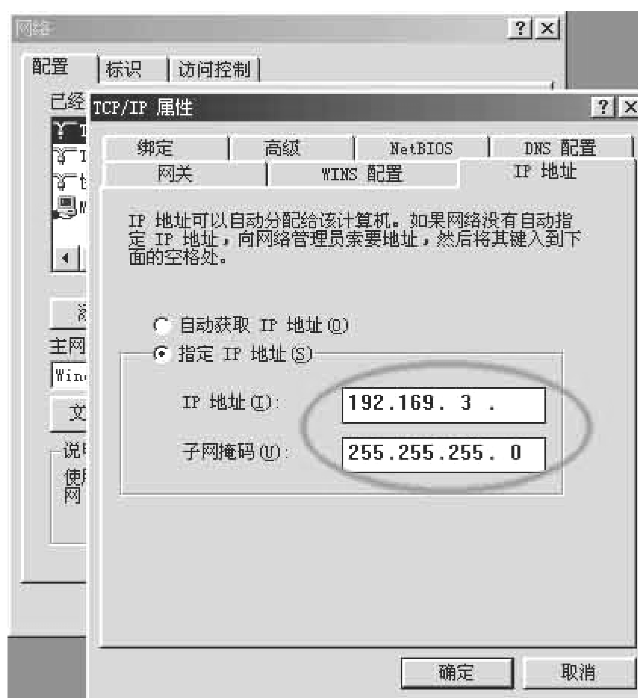
注：这里的工作站指的是要内网的 WINDOWS98/NT **等。**

WINDOWS98 工作站设置举例

用鼠标点按 WINDOWS **桌面下方的**[**开始**]**，选取**[**设置**]**，**[**控制面板**]**，**

用鼠标双击[**网络**]**图标，出现有关网络配置的对话框，找出网卡对应的的** TCP/IP **对应的项并点按**[**属性**]。**如果这里没有网卡或** TCP/IP **选项，按下面的**[**添加**]**加入要应项。**

点按属性后，出现如下的对话框，有其[IP **地址**]**中写入分配给这个工作站的** IP **地址，和子网掩码**(**子网掩码我们一般定为：**255.255.255.0).



转入[**网关**]**，填入** APN GW **的内部** IP **地址。在** 'DNS '**中添加本地** ISP **的** DNS **地址。然后请点击** '**确定** '**按钮以保存输入的数据。并按计算机给出的提示重新启动工作站。重新启动后即可上网。工作站可以按正常使用上网的方式来使用互联网，也可以使用内部的虚拟网。**

提示：如果您的 APNGW **启动了** DHCP/DNS **服务，您可以采用自动获得** IP **地址的选项。这样网卡就不需要任何其他的设置。**

第五章 常见问题解答

本章列举了部分常见的问题。更多信息，可以参考我们的网站。

客户机不能被代理上网

1. 检查是否连接 Internet。直接在 apn 上 ping 公网 IP 即可。例如 202.96.134.133。
2. 如 APN 能上网而客户机不能，请检查 Licenses 是否设置正确。
3. 如果以上都正确，请检测网络物理连接；

如何判断是 APN 硬件故障还是网络故障？

1. 检查 APN 的自检灯是否正常。1000、2000 为常亮。如果不亮表示硬件有故障；
2. 检查网络是否接触良好。正确情况下网卡指示灯会亮；
3. 检查是否能进入 APN 的 console 配置模式；
4. 以上都正常表示硬件工作正常。可以进一步通过日志查看系统信息。

如何知道有那些机器相连

1. 运行 ***route −n***，可以看到其他机器的列表（以 IP 地址表示）。
2. 在 GW2000 以上机器中，可以通过 ***ipsec auto status*** 查看详细的隧道建立的信息。

MODEM 不自动拨号

1. 检测电话线是否正常。
2. MODEM 与电脑联接的串口线松动。
3. Modem 是否掉电。

MODEM 能拨号，但总不通

1. 查看是否有他人在使用与 APN GW 相同的上网帐号。
2. 查看这个帐号是否过期。

ADSL 无法拨号上网

1. 首先检测您的网线是否使用正确。大多数 ADSL modem 使用普通网线直接与 APN GW 的 WAN1 相连。
2. 检测您的用户名和帐户是否正确或备盗用。一定要按照 ISP 给您的用户名和帐户输入。
3. 部分地区的 ADSL 用户，在终端设备突然掉电之后，不能马上拨号。需要等待一会才能重新连接。
4. 您可以在[APN GW/]模式下输入 ***adsl-start*** 重新连接。同样有效的命令还有 ***adsl-stop***, ***adsl-status***（查看状态）

不能启动

1. 查看电源是否工作。如果正常，前面板的电源指示灯应该亮绿。
2. 查看 APN 前面板的系统自检灯是否正常。如果没有指示，说明是系统硬件故障，您需要与供应商或维修中心联系更换。

APN 连接 Internet 前可以进入监管界面，但后来局域网工作站不能上网，也不能进入监管界面

1. **检测同组内的子网与其它同组网内的网络地址相同，发生冲突。同一个** vdomian **内不同** vhost **的的机器不能在同样一个网段。**

如何查看我现在 APN 的公网 IP 地址？

在 web **配置模式下，点击基本网络，可以看到现在的公网** IP **地址。**

在 console **或** telnet **模式下，**

您可以使用 ifconfig **查看：**

```
ifconfig
…….
ppp0        Link encap:Point-to-Point Protocol
            inet addr:218.17.67.147   P-t-P:218.17.65.1   Mask:255.255.255.255
            UP POINTOPOINT RUNNING NOARP MULTICAST   MTU:1492   Metric:1
           RX packets:766024 errors:0 dropped:0 overruns:0 frame:0
           TX packets:548002 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0
```

本例显示的 218.17.67.147 **是此时** APN **公网的** IP **地址。**

如果您是 ADSL **连接** Internet**，您可以使用** adsl-status **查看当前的** IP **地址。**

```
[APN GW/]adsl-status
adsl-status: Link is up and running on interface ppp0
ppp0        Link encap:Point-to-Point Protocol
            inet addr:218.17.67.147   P-t-P:218.17.65.1   Mask:255.255.255.255
            UP POINTOPOINT RUNNING NOARP MULTICAST   MTU:1492   Metric:1
           RX packets:766486 errors:0 dropped:0 overruns:0 frame:0
           TX packets:548359 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0
```

如何打开 Telnet 让远程技术人员登录

您可以使用

[APN GW/]***advconf telnet start***

打开 Telnet **功能。此时您可以查看当前** APN **的公网地址，这样就可以让远程的技术人员登录** APN **进行调试。**

注意您如果需要一直打开 telnet **功能，需要记住更改您的密码。**

同时您还需要把访问许可中，启动允许外网访问。否则只能从内外 Telnet**。**

我的 ADSL 线路不是很稳定，常常锁定怎么办？

APN **支持一个心跳检测功能，可以设定每段时间后自动检测是否在线。如果发现锁住，会自动重连** Interent**。考虑系统资源消耗的问题，标配** APN **都没有该模块。如您需要可与我们联系。**

我原来就有 DDN 线路，新的节点的扩展能够用 APN 吗？

APN 可以和原来的线路（专线、VPN）等无缝的连接在一起。这需要了解您的网络的具体情况。如您需要请与我们联系。

我的上网方式被 MAC 地址绑定了，怎么办？

APN 甚至支持修改网卡的 MAC 地址。

APN 可以放在防火墙之后吗？

一般说来，放在任何位置都是可以的。但如果是放在防火墙之后，您需要确认您的防火墙可以透转 IPSec 或 GRE 协议才可。

我两边都是 ADSL，通讯带宽有多少？

ADSL 是非对称的，一般是上行 512K，下行 2M-4M。通讯时只能在最小值之间平等通讯，所以一般两条上行 512K、下行 4M 的 ADSL 通讯，VPN 隧道的带宽理论值是 512K。

APN 支持带宽管理吗？

APN 支持带宽管理，可以设置非常灵活的策略。由于设置比较灵活，需要结合您的具体情况。请与我们联系。

我忘记了密码怎么办？

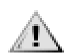
如果您不巧忘记了自己的口令，APNGW 提供一个 Rescue Mode，可以不用口令登录。这需要使用者直接接触到 APN，通过其配置的 console 线来恢复口令。

在用控制台进入 APNG 配置之中，其中会有一个信息：

Press R with 3 seconds enter rescue mode. Configuring and Starting LAN Network........

这时候会有一个 3 秒的时间您可以通过按 R 键和缺省口令登录 APNGW。登录之后，您可以更改您的口令或增加新的用户名和口令。

警告：



如果您改变了您的 root 密码而不巧将其忘记的话，您可以使用安全模式进入 APNGW。该模式不可以远程操作。
